Abstract of the Disclosure

A method authenticates d_i identities in parallel using two prime numbers p and q such that $q \mid p - 1$. Each identity includes a private key s_i and a public key v_i, and a publicly known generator is α such that $\alpha^q \equiv 1\ (mod\ p)$,. A verifier is provided with an ordered list of the public keys v_i. A prover selects uniformly at random a non-negative number r less than q. A number $x = \alpha^r\ (mod\ p)$ is sent from the prover to a verifier. The verifier selects uniformly at random a non-negative number e less than $2^{(t+logd)}$, where log is base 2, and a number t is a predetermined security parameter. The prover receives from the verifier the number e. A number $y = r + \Sigma_i\, s_i * e^i\ (mod\ q)$ is generated by the prover, and the number Y is sent to the verifier, who then determines if an equality $x = \alpha^y * \Pi_i (v_i)^{e^i}\ (mod\ p)$ is true. The prover is accepted as having the d_i identities if and only if the equality is true. In a preferred embodiment the communications between the prover and the verifier is via a low-bandwidth optical channel.